In the Claims:

Please amend Claims 1 and 6-12, and add new Claims 16-18, as indicated below. The status of all pending claims is as follows:

1. (Currently Amended) A magnetic disk apparatus comprising:

a cipher key memory unit which stores a single cipher key used for encoding and decoding data;

a cipher encode unit which encodes data input via an interface from an upper apparatus using the cipher key stored in said cipher key memory unit, the cipher encode unit recording the encoded data onto a magnetic disk medium;

a cipher decode unit which decodes the encoded data read out from the magnetic disk medium using the cipher key stored in said cipher key memory unit, the cipher decode unit outputting the decoded data via the interface to the upper apparatus; and

a cipher key change unit which erases said cipher key stored in said cipher key memory unit, defined as a first cipher key, and ~~replaces~~ overwrites the first cipher key with another cipher key, defined as a second cipher key, which cannot decode the encoded data recorded on the magnetic disk medium;

wherein the cipher key change unit ~~replaces~~ overwrites the first cipher key stored in said cipher key memory unit with the second cipher key in response to a command for discarding all of a first encoded data recorded on the magnetic disk medium, and makes

decoding the first encoded data impossible, the first encoded data encodes using the first cipher key stored in said cipher key memory unit.

2. (Previously Presented) The magnetic disk apparatus according to claim 1, wherein

the cipher key memory unit stores a predefined cipher key written at a stage of manufacturing the apparatus.

3. (Original) The magnetic disk apparatus according to claim 1, wherein the cipher key memory unit is a nonvolatile memory.

4. (Currently Amended) The magnetic disk apparatus according to claim 1, wherein

the cipher key memory unit is a medium area other than a user recording area of the magnetic disk medium.

5. (Cancelled)

6. (Currently Amended) The magnetic disk apparatus according to claim 1, wherein

the cipher key change unit ~~replaces~~ overwrites the cipher key in the cipher key memory unit in response to a special command other than a command system for the upper apparatus.

7. (Currently Amended) The magnetic disk apparatus according to claim 1, wherein

the cipher key change unit ~~replaces~~ overwrites the cipher key in the cipher key memory unit in response to a special command from a cipher key change application installed in the upper apparatus.

8. (Currently Amended) The magnetic disk apparatus according to claim 1, wherein

the cipher key change unit ~~replaces~~ overwrites the cipher key in the cipher key memory unit in response to a special command from a cipher key change application installed by the upper apparatus via a network.

9. (Currently Amended) The magnetic disk apparatus according to claim 1, wherein

the cipher key change unit ~~replaces~~ overwrites the cipher key in the cipher key memory unit by recognizing a physical event manipulation in the apparatus.

10. (Currently Amended) The magnetic disk apparatus according to claim 1, wherein

the cipher key change unit ~~replaces~~ overwrites the cipher key by generating a new cipher key through a process of shuffling of the cipher key stored in the cipher key memory unit.

11. (Currently Amended) The magnetic disk apparatus according to claim 1, wherein

the cipher key change unit ~~replaces~~ overwrites a cipher key stored in the cipher key memory unit into another cipher key added to a cipher key change command from the upper apparatus.

12. (Currently Amended) A cipher processing method for a magnetic disk apparatus, comprising:

a cipher key memory step of storing in a cipher key memory unit a single cipher key used for encoding and decoding data;

an encoding/recording step of converting data input via an interface from an upper apparatus into encoded data using the cipher key stored in said cipher key memory unit, and recording the encoded data onto a magnetic disk medium;

a decoding/readout step of decoding the encoded data read out from the magnetic disk medium using the cipher key stored in the cipher key memory unit, and outputting the decoded data via the interface to the upper apparatus; and

a cipher key change step of erasing said cipher key stored in said cipher key memory unit, defined as a first cipher key, and ~~replacing~~ overwriting the first cipher key with another cipher key, defined as a second cipher key, which cannot decode the encoded data recorded on the magnetic disk medium;

wherein the cipher key change step includes ~~replacing~~ overwriting the first cipher key stored in said cipher key memory unit with the second cipher key in response to a command for discarding all of a first encoded data recorded on the magnetic disk medium, and making decoding the first encoded data impossible, the first encoded data encodes using the first cipher key stored in said cipher key memory unit.

13-15. (Cancelled)

16. (New) The cipher processing method according to claim 12, wherein said command for discarding all of the first encoded data recorded on the magnetic disk medium is a command from the upper apparatus.

17 (New) The magnetic disk apparatus according to claim 1, wherein after the cipher key change unit overwrites the fist cipher key with a second cipher key, functions of the magnetic disk apparatus are not lost and the magnetic disk apparatus can be reused.

18. (New) The cipher processing method according to claim 12, wherein after said cipher key change step is performed, functions of the magnetic disk apparatus are not lost and the magnetic disk apparatus can be reused.